AO93 Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of:	Case No. 23-6160MB
12607 W. Vista Paseo Dr., Litchfield Park, AZ 85340 and the person of Christina Marie Chapman.	[redacted]

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona:

As further described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

As set forth in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before November 8, 2023 *(not to exceed 14 days)*
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the District of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized ☐ for 30 days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: October 25, 2023@6:30pm _____
Judge's signature

City and state: Phoenix, Arizona

Honorable Alison S. Bachus, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The property and places to be searched are:

(1) 12607 W Vista Paseo Dr., Litchfield Park, Arizona, 85340. The residence is a one-story, single-family home with a tan and beige stucco exterior, and tile roof. A photograph of the residence is included below.

(2) The person of Christina Marie Chapman, pictured below, having SSN [redacted]7030 and DOB [redacted]975.

ATTACHMENT B

Property to be seized

1. All records relating to violations 18 U.S.C. §§ 1956 (laundering of international monetary instruments), 1960 (unlicensed money transmitting business), and 8 U.S.C. § 1324 (unlawful employment of aliens), and occurring in or after January 2021, including:

   a. records and information relating to a conspiracy to defraud entities seeking to employ remote workers;

   b. records and information relating to a conspiracy to launder funds to and from the United State to and from a location outside the United States;

   c. employment records of remote workers and Christina Marie Chapman;

   d. financial records of remote workers and Christina Marie Chapman;

   e. personal identification documents for Christina Marie Chapman;

   f. records and information relating to the location of participants in a scheme to defraud U.S.-based entities seeking to employ remote workers;

   g. records and information relating to Company 1 COMPANY 2 COMPANY 3 COMPANY 3 COMPANY4 COMPANY 5 COMPANY6 COMPANY6 , COMPANY 7 COMPANY 8 COMPANY 9 COMPANY 10 COMPANY 11 COMPANY 11 COMPANY 7 COMPANY 12 COMPANY 12 COMPANY 13 [redacted] [redacted] [redacted] Capital One Financial, Wells Fargo, Individual 2 Individual 5 Individual 5 Individual 1 Individual 3 Individual 6 Individual 3 Individual 8

[redacted] PayPal, Payoneer, Dedipath, GitHub, and CashApp;

h. records and information related to individuals gaining employment as a remote worker;

i. records and information related to U.S.-based entities who employed remote workers;

j. records and information relating to the scheme to employ remote workers that are found in email accounts: [redacted] and [redacted]

k. records and information relating to the identity or location of the remote workers; and

l. records and information relating to malicious software.

2. Books, records, receipts, notes, ledgers, invoices, and any other documentation related to the scheme;

3. Notes containing the individual names of such persons, telephone numbers or addresses of associates in the schemes, and any records of accounts receivable, money paid or received, cash or checks received, or intended to be paid;

4. VOIP equipment and service documents;

5. Records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, cashier's checks, check stubs, PayPal, Payoneer, or other electronic money transfer services, check or money order purchase receipts, account statements, and any other records reflecting the receipt, deposit, or transfer of money;

6. United States currency, foreign currency, and receipts or documents regarding purchases of real or personal property;

7. Safe deposit box keys, storage locker keys, safes, and related secure storage devices, and documents relating to the rental or ownership of such units;

8. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises and any vehicles found thereon during the execution of the warrant, including, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, records of real estate transactions, vehicle titles and registration, and vehicle maintenance records;

9. Photographs, including still photos, negatives, slides, videotapes, and films, in particular those showing co-conspirators, criminal associates, U.S. currency, real and personal property;

10. Computers, cellular phones, tablets, and other media storage devices, such as thumb drives, CD-ROMs, DVDs, Blu Ray disks, memory cards, and SIM cards (hereafter referred to collectively as "electronic storage media");

11. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

12. Any records and information found within the digital contents of any electronic storage media seized from the Subject Premises, including:

a. all information related to the offenses as described in paragraph 1;

b. all bank records, checks, credit card bills, account information, or other financial records;

c. any information recording schedule or travel;

d. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, and phonebooks;

e. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use,

and events relating to crime under investigation and to the electronic storage media user;

f. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;

g. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;

i. evidence of the times the electronic storage media were used;

j. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;

k. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;

l. records of or information about Internet Protocol addresses used by the electronic storage media;

m. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;

n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or

other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

This warrant authorizes a review of records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.